NED CAREY
Legislative District 31A
Anne Arundel County

Economic Matters Committee

Subcommittees

Alcoholic Beverages
Chair, Unemployment Insurance

House Chair
Joint Committee on
Unemployment Insurance Oversight

Chair
Anne Arundel County Delegation

THE MARYLAND HOUSE OF DELEGATES
ANNAPOLIS, MARYLAND 21401

The Maryland House of Delegates
6 Bladen Street, Room 161
Annapolis, Maryland 21401
410-841-3047 · 301-858-3047
800-492-7122 *Ext.* 3047
Ned.Carey@house.state.md.us

HB 888 - Consumer Protection - Security Features for Connected Devices

SPONSOR TESTIMONY

Cross-file: SB 443

House Economic Matters Committee, February 26, 2020

Chairman Davis, Vice Chair Dumais and Members of the Committee,

House Bill 188 is an "Internet of Things" (IoT) cybersecurity bill, requiring manufacturers of internet connected devices to equip such devices with reasonable security features to protect against ransomware attacks, data theft, cyber-stalking and other forms of cyber intrusion.

"Internet of Things" simply refers to connected devices – physical objects capable of connecting to the internet. These smart devices are mostly in our homes and include TVs, refrigerators, home security systems, thermostats and sensors of all types which can be easily hacked with default passwords, and weaponized or otherwise sabotaged.

These devices add convenience and entertainment to our lives – Alexa-enabled Echo and Ring are just a few well-known examples. They even bring health benefits and energy savings to occupants and owners of Smart Environments through regulation of thermostats, ready access to health information and personalized services.

Unfortunately, the video you've just seen in this hearing shows us how vulnerable we are if these devices are not properly secured. In case you missed it: https://youtu.be/VuKNq7UM1v0

Guidelines from the Federal Communications Commission recommend that the manufacturer of an internet connected device create a "reasonable security feature" for that device. Within that guidance, this bill codifies best practices for cybersecurity protections for connected devices, and clarifies that adopting a unique code for each device is a reasonable security feature to satisfy the policy intent of the FCC guidance.

Simply put: These devices need to be manufactured either with a unique code, or with the feature that allows the purchaser to create a password of their own choosing.

California passed a similar law in 2018, and Oregon has a bill that has also been enacted. Legislation is currently being introduced in Illinois and by our neighbors in Virginia.

We want to continue to enjoy the benefits of these devices and future innovations. In order to do so in a safe environment, they need to be designed properly to reduce the potential for harm. Cyberattacks and data breaches are a threat to consumer privacy, public safety, and national security. Manufacturers have a social responsibility to equip the devices they produce with security features that provide a reasonably effective defense in the 21st century digital environment. This bill codifies that responsibility and levies penalties on manufacturers that fail to uphold that responsibility.

For this reason, I ask for a favorable report on HB 888.